NSCB1418BCN

vmware EXPLORE

Best Practices for Hardening Your VMware Infrastructure

Daniel Mazzini

Sr Staff Architect,
VMware

Kacy Reed

Staff Architect,
VMware

#vmwareexplore #NSCB1418BCN

Required Disclaimer

This presentation may contain product features or functionality that are currently under development.

This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.

Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.

Technical feasibility and market demand will affect final delivery.

Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

Presenters

Daniel Mazzini

Sr Staff Architect

Kacy Reed

Staff Architect

Agenda

The Path to Securing Your Infrastructure

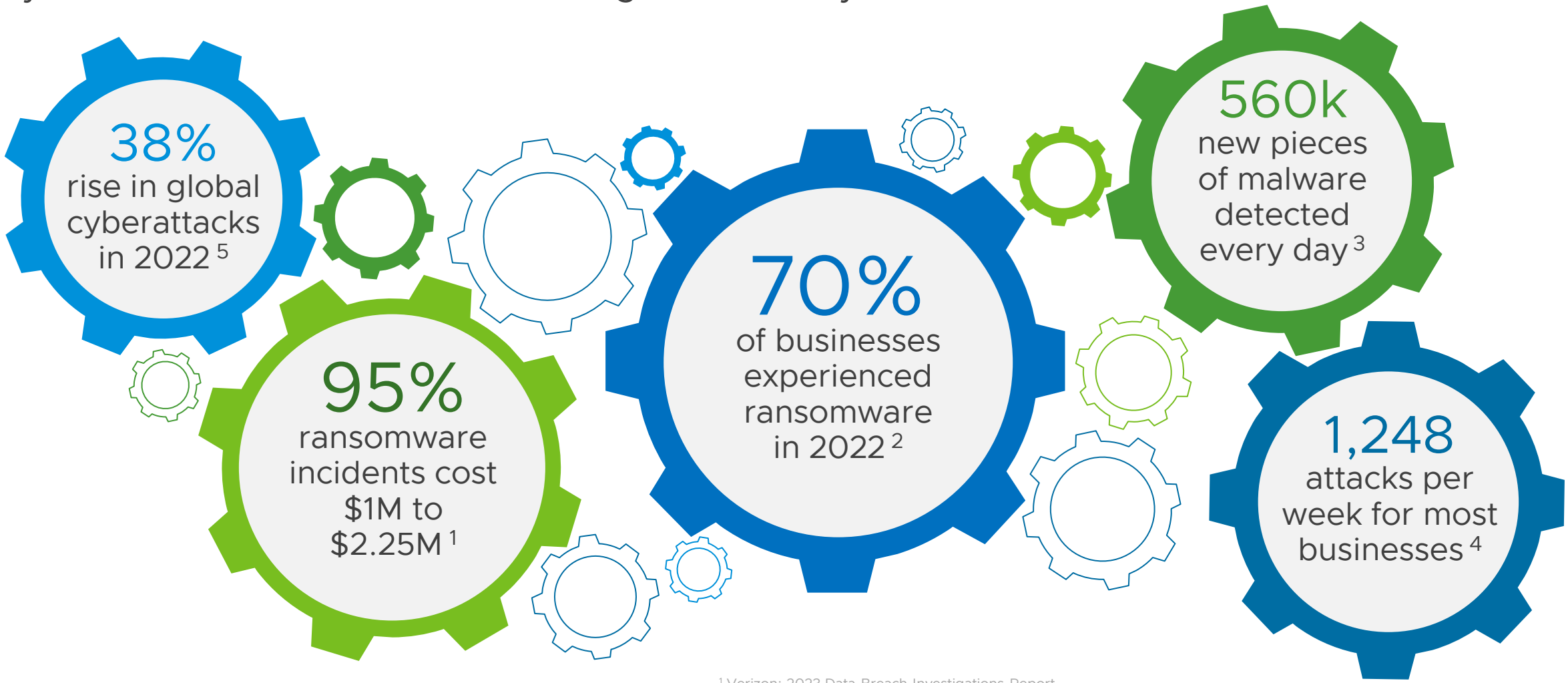
Best Practices for VMware Products

Resources

Q & A

Why Prioritizing a Secure Infrastructure Can't Wait

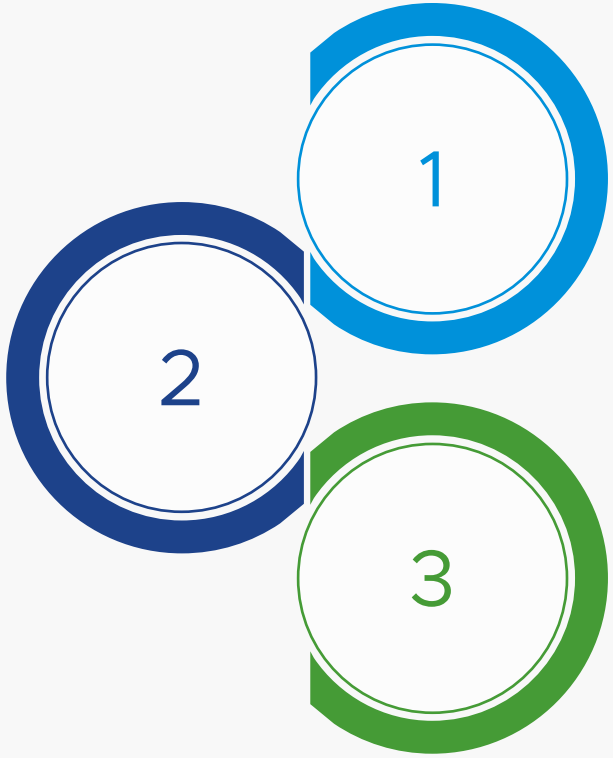
Cyber attackers and threat actors target data everywhere – all the time



[1] Verizon: 2023 Data Breach Investigations Report
[2] www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
[3] https://dataprot.net/statistics/malware-statistics/
[4] https://pages.checkpoint.com/forrester-wave-for-enterprise-email-security-2023.html
[5] https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks

The Steps to Securing Your Infrastructure

Define your future-state cybersecurity strategy



Evaluate your current security state

Harden your VMware environment

Assess and Evaluate Your Current State

Assessment outcomes include a plan to reach your target state

Assessment Practices

Identify and evaluate threats, vulnerabilities, risks, compliance requirements, and effectiveness of existing security controls

Suggested frequency:
Once every two years
depending on industry and regulatory compliance requirements or when major architecture changes occur

Assessment Outcomes

- Gaps in current state security posture identified
- Recommendations for remediation and mitigation
- Action plan for remediation to achieve target state
- Compliance with regulations and standards
- Improvement of overall security posture

The Assessment Process

High-level evaluation process and defining the future state

Step 1
Determine assessment scope
Define scope, identify assets to assess, and establish objectives and criteria

Step 2
Information gathering
Collect VMware infrastructure data and information on hardware, software, and network

Step 3
Analysis
Align to a cybersecurity framework for review of current state and to define target of future state

Step 4
Reporting and roadmap
Document assessment findings and recommendations and create a roadmap to mitigate gaps

Step 5
Remediation
Perform remediation of vulnerabilities and implement mitigating controls

Step 6
Follow up
Monitor infrastructure over time for effectiveness of remediation and for new risks

Security Assessments Must Cover the Entire IT Ecosystem

Infrastructure security

Underlying infrastructure
- Network
- Servers
- Storage
- Virtualization layer

Additional areas
- Access controls
- Patch management
- Security configurations

Compliance

Evaluations for meeting regulatory requirements and industry best practices
- Infrastructure
- Virtual machines
- Applications

Virtual machine security

Security controls effectiveness
- Firewalls
- Intrusion detection/ prevention systems
- Advanced threat prevention
- Anti-malware software
- VM template/ image mgmt
- VM encryption

Disaster recovery and business continuity

Evaluations for adequate recovery and business continuity plans in the event of a breach, attack, or disruption

Application security

Access controls effectiveness
- Authentication mechanisms
- Encryption
- Input validation
- Intrusion detection/ prevention systems
- Advanced threat prevention

Governance, risk, and compliance (GRC)

Evaluations for the effectiveness of the organization's GRC processes
- Risk management
- Policy management
- Compliance monitoring

Implementing Security Best Practices to Harden Your Infrastructure

Hardening outcomes reduce potential for cyber attacks and data breaches

Hardening Practices

Secure VMware infrastructure by implementing best practices aligned to an industry-recognized cybersecurity framework

Suggested frequency:
During initial implementation and throughout system life cycle until end-of-life decommissioning

Hardening Outcomes

- Improved access controls
- Strengthened network security
- Reduced attack surfaces
- Better performance
- Simplified compliance

The Hardening Process

High-level process to help achieve the desired future state

Step 1
Determine scope and identify risks
Review security policies, standards, and architecture

Step 2
Develop a security plan
Set the standard for baseline configurations aligned to a cybersecurity framework

Step 3
Implement security controls
Implement configuration and security controls and test performance to ensure validity

Step 4
Monitor and assess security
Ensure compliance with continuous third-party monitoring and periodic assessments

Step 5
Maintain and update controls
Keep software up-to-date to remain vigilant for new vulnerabilities and threats

Step 6
Follow up
Monitor infrastructure over time for effectiveness and review each time it changes

Best Practices for Security Hardening

Security hardening

- Disable unnecessary services
- Apply security patches
- Configure host-based firewalls

Network hardening

- Configure network devices
- Configure and implement VLANs, access control lists, and network segmentation

Virtual machine hardening

- Configure virtual machines (VMs) running on VMware infrastructure
- Apply security patches to VMs
- Disable unnecessary services
- Configure firewalls on VMs

Access control

- Implement access controls to limit access for VMware infrastructure to authorized users
- RBAC, strong authentication on mechanisms
- Least privilege access

Encryption

- Implement SSL/TLS encryption for network traffic
- Encrypt VM disks and virtual hard disks

Monitoring and logging

- Implement monitoring and logging mechanisms
- Implement IDS/IPS and advanced threat prevention (ATP)
- Implement security information and event management (SIEM) tools

VMware vSphere® Hardening Best Practices Checklist

Virtual machines

- ❑ UEFI secure boot
- ❑ Removable device controls
- ❑ Minimize use of VM console
- ❑ Deactivate host-guest file system (HGFS)
- ❑ Disable copy and paste, drag and drop
- ❑ Restrict API access
- ❑ vMotion encryption

ESXi hosts

- ❑ UEFI secure boot
- ❑ Enable lockdown mode
- ❑ Disable SSH
- ❑ VIB acceptance levels
- ❑ Disable SLP
- ❑ CIM access levels
- ❑ Host firewall
- ❑ Disable SNMP

VMware vCenter®

- ❑ Management session restrictions
- ❑ Disable managed object browser
- ❑ Restrict cryptographic role and permissions
- ❑ SSO account alerting and restrictions
- ❑ Enable TLS 1.2
- ❑ PowerCLI restrictions
- ❑ VMware vCenter server firewall
- ❑ Use approved certificates
- ❑ Use templates to deploy VMs
- ❑ Use SNMP v3

Virtual network

- ❑ vMotion network isolation
- ❑ ESXi management isolation
- ❑ VMware vSphere web client isolation
- ❑ Isolate virtual machine traffic

Hardening practices for all areas and products

Patch currency

- ❑ Install latest security patches and updates

Identity and access management

- ❑ Disable default accounts
- ❑ Change default passwords
- ❑ RBAC
- ❑ Centralized authentication
- ❑ Multi-factor authentication
- ❑ Single sign-on
- ❑ Account lockout
- ❑ Unique service accounts

Remote logging

- ❑ Enable logging to appropriate levels
- ❑ Forward logs to centralized log collector
- ❑ Limit access to logs

Monitoring

- ❑ VMware Aria™
- ❑ VMware vCenter server alerts
- ❑ Third-party tool

Backups

- ❑ Ensure environment is backed up

VMware Cloud Foundation™ Hardening Best Practices Checklist

VMware vSphere® checklist

- ❑ All items on VMware vSphere hardening checklist (previous slide) for virtual machines, ESXi hosts, VMware vCenter, and virtual network

VMware NSX®

- ❑ VMware NSX (formerly VMware NSX-T™ Data Center) deployment protocol and port requirements
- ❑ VMware NSX® Manager™ appliance deployment
- ❑ VMware NSX® Edge™ appliance deployment
- ❑ VMware NSX logs and alerting*

* More details on VMware NSX hardening checklist

VMware vSAN™

- ❑ VMware vSAN network isolation
- ❑ Enable VMware vSAN encryption

VMware Cloud Foundation™ SDDC Manager™

- ❑ VMware Cloud Foundation SDDC Manager isolation
- ❑ Use approved certificates
- ❑ Use dedicated account for updates and patches
- ❑ Deploy with FIPS mode enabled
- ❑ Schedule automatic password rotation

Hardening practices for all areas and products

Patch currency

- ❑ Install latest security patches and updates

Identity and access management

- ❑ Disable default accounts
- ❑ Change default passwords
- ❑ RBAC
- ❑ Centralized authentication
- ❑ Multi-factor authentication
- ❑ Single sign-on
- ❑ Account lockout
- ❑ Unique service accounts

Remote logging

- ❑ Enable logging to appropriate levels
- ❑ Forward logs to centralized log collector
- ❑ Limit access to logs

Monitoring

- ❑ VMware Aria™
- ❑ VMware vCenter server alerts
- ❑ Third-party tool

Backups

- ❑ Ensure environment is backed up

VMware NSX® Hardening Best Practices Checklist

Protocols and Port Requirement

- ❑ Follow TCP/UDP port guidelines
- ❑ Block unneeded ports
- ❑ Disable unneeded network services

VMware NSX® Manager™ (Management Plane)

- ❑ VMware NSX Manager isolation
- ❑ VMware NSX® Controller™ isolation
- ❑ VMware NSX transport node isolation
- ❑ Management session restrictions
- ❑ SSH access to NSX Manager disabled
- ❑ Ensure that NTP server is authorized
- ❑ Do not install/use software unsupported by VMware
- ❑ Use SFTP for backup and restoration
- ❑ Hardening IAM policies in NSX cloud service environment
- ❑ Set NSX Manager WEB/API access using only TLS 1.2
- ❑ Disable SNMP v2
- ❑ Use approved certificates
- ❑ Password retention policy

VMware NSX Edge™ (Data Plane)

- ❑ Block access to ports not used on data plane
- ❑ Segment management and data traffic
- ❑ Isolate storage network from other networks
- ❑ Disable secure shell
- ❑ Isolate virtual network tunnel traffic (Geneve)

VMWare NSX® Certificates

- ❑ Ensure that NSX Manager certificate is valid and legitimate
- ❑ Leverage VMware NSX® Edge™ certificates and cipher suites (load balancer, IPSec, and VPN)
- ❑ User access to NSX Manager using own certificate authority

VMware NSX® Distributed Firewall™

- ❑ Implement micro-segmentation with NSX Distributed Firewall
- ❑ Implement NSX Distributed Firewall with Threat Prevention
- ❑ Implement NSX Distributed Firewall with VMware NSX® Advanced Threat Prevention™

VMware NSX® Gateway Firewall™

- ❑ Enforce security policies
- ❑ Implement NSX Gateway Firewall with Threat Prevention
- ❑ Implement NSX Gateway Firewall with Advanced Threat Prevention

\+ Hardening practices for all areas and products

vmware®

Hardening Resources on VMware.com

VMware Hardening Guides	These guides provide prescriptive guidance for customers on how to deploy and operate VMware products in a secure manner. Find them at https://www.vmware.com/security/hardening-guides.html.
VMware Cloud Foundation™ Compliance Kits	These kits help customers meet regulatory requirements by bridging the gap between compliance frameworks and implementation guides. Find them at https://core.vmware.com/compliance#cloud-foundation.
Secure Technical Implementation Guides	VMware supports the mission of the U.S. Department of Defense through security technical implementation guides – a collaborative effort between VMware and the Defense Information Systems Agency. Find them at https://core.vmware.com/stigs.
Product Audit and Applicability Guides	Implementation guides to assist administrators in implementing security controls for a specific compliance framework as well as helping auditors understand how product security controls apply to regulatory requirements. Find them at https://core.vmware.com/compliance.
VMware Firewall Ports and Protocols	This is a complete list of ports required for VMware products to be able to create dynamic lists based on the VMware products in your environment. Find them at https://ports.esp.vmware.com.
VMware Security Advisories	Stay up-to-date on the latest VMware security advisories and updates. Find them at https://www.vmware.com/security/signup-for-advisories.html.

Q & A

vmware EXPLORE

Thank You